Distributed Reed-Solomon Codes for Simple Multiple Access Networks

Wael Halbawi, Tracey Ho
Department of Electrical Engineering
California Institute of Technology
Pasadena, California 91125
Email: {whalbawi,tho}@caltech.edu

Hongyi Yao
Oracle Inc.
400 Oracle Parkway
Redwood City, California 94065
Email: yaohongyi03@gmail.com

Iwan Duursma
Department of Mathematics
University of Illinois
Urbana, Illinois 61801
Email: duursma@math.uiuc.edu

Abstract

We consider a simple multiple access network in which a destination node receives information from multiple sources via a set of relay nodes. Each relay node has access to a subset of the sources, and is connected to the destination by a unit capacity link. We also assume that z of the relay nodes are adversarial. We propose a computationally efficient distributed coding scheme and show that it achieves the full capacity region for up to three sources. Specifically, the relay nodes encode in a distributed fashion such that the overall codewords received at the destination are codewords from a single Reed-Solomon code.

I. Introduction

We consider a simple multiple access network in which a single destination node wishes to receive information from multiple sources via a set of relay nodes, each of which has access to a subset of the sources. Each relay node is connected to the destination by a unit capacity link. Our objective is to design a distributed code that can correct arbitrary adversarial errors on up to z links (or, equivalently, relay nodes). This problem has been considered previously by [1] in the context of decentralized distribution of keys from a pool, where it was shown to be a special case of the general multiple access network error correction problem, whose capacity region was established in [2]. It can also apply to other distributed data storage/retrieval scenarios where different nodes store different subsets of the source messages.

In this paper, we propose a computationally efficient coding scheme, distributed Reed-Solomon codes, for simple multiple access networks. In particular, the relay nodes encode in a distributed fashion such that the overall codewords received at the destination are codewords from a single Reed-Solomon code, which allows the destination

This work was partially supported by the Qatar Foundation - Research Division (supporting the work of Wael Halbawi), NSF Grant CNS-0905615 (supporting the work of Tracey Ho and Hongyi Yao), and a grant from the Simons Foundation (#280107 to Iwan Duursma). The work of Hongyi Yao was done while he was at the California Institute of Technology.

to decode efficiently using classical single-source Reed-Solomon decoding algorithms. This scheme obviates the need for encoding over successively larger nested finite fields at each source as in the prior construction of [2]. We prove that the proposed coding scheme achieves the full capacity region for such networks with up to three sources.

A. Related work

A related problem was studied in [3], where the authors construct MDS codes with sparse generator matrices, motivated by sensor networks in which a group of distributed sensors collectively measure a set of conditions (sources). Unlike the scenario we study, in [3] it is assumed that each sensor has access to all sources and can choose which ones to measure, and the issue of decoding complexity is not addressed.

Another related problem is the Coded Cooperative Data Exchange Problem considered in [4]. Like our problem, each node has a subset of messages, but unlike our problem, the nodes communicate cooperatively via error-free broadcast transmissions in order to disseminate all messages to all nodes.

II. System model and Background

A Simple Multiple Access Network (SMAN) is defined as follows. A single destination node D wishes to receive information from multiple source nodes $\mathcal{S} = \left\{S_1, S_2, \ldots, S_{|\mathcal{S}|}\right\}$ via a set of intermediate relay nodes $\mathcal{V} = \{v_1, \ldots, v_N\}$. The information rate of each source $S_i \in \mathcal{S}$ is denoted by r_i. Each relay node has access to a subset of sources, or equivalently, each source $S_i \in \mathcal{S}$ is connected to a subset of relay nodes by *source* links of capacity r_i. Each relay node $v_i \in \mathcal{V}$ is connected to D by a link of unit capacity. We refer to these links as *relay* links. We wish to correct arbitrary or adversarial errors on up to z relay links or equivalently nodes. An example of a SMAN is given in Figure 1.

An adjacency matrix $\mathbf{A}$ is associated with a SMAN, where the rows and columns represent $\mathcal{S}$ and $\mathcal{V}$, respectively, and $\mathbf{A}_{i,j} = 1$ if there exists a source link connecting S_i to v_j.

Let $\mathcal{I}(\mathcal{S}')$ denote the index set of elements in $\mathcal{S}'$, i.e. $\mathcal{I}(\mathcal{S}') = \{i : S_i \in \mathcal{S}'\}$. Also define $\mathcal{I} := \mathcal{I}(\mathcal{S})$ and $r_{\mathcal{I}(\mathcal{S}')} := \sum_{i \in \mathcal{I}(\mathcal{S}')} r_i$. The minimum cut capacity (min-cut) from $\mathcal{S}'$ to D is denoted by $C_{\mathcal{I}(\mathcal{S}')}$, $\forall \mathcal{S}' \subseteq \mathcal{S}$. Note that $C_{\mathcal{I}} = N$. From [2], the capacity region $\mathcal{R}$ of a SMAN is given by cut set bounds for each subset of sources, i.e. the capacity region is the set of all rate vectors $\mathbf{r} = \left(r_1, r_2, \ldots, r_{|\mathcal{S}|}\right)$ such that

$$r_{\mathcal{I}(\mathcal{S}')} \leq C_{\mathcal{I}(\mathcal{S}')} - 2z, \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{1}$$

Furthermore, it suffices to carry out linear network coding at internal network nodes, where each v_i transmits linear combinations of received symbols over $\mathbb{F}_q$.

III. Preliminaries

To construct a distributed Reed-Solomon code for the above-described SMAN with N intermediate relay nodes and z adversarial nodes, we start with an $[N, k, d]_q$ Reed-Solomon code where $d = 2z + 1 = N - k + 1$. For the purpose of this work, we will use the definition of a Reed-Solomon Code as in [5]. This is a k-dimensional

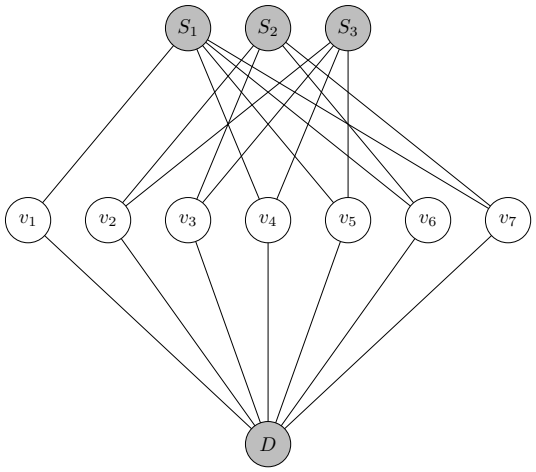

Fig. 1. An example of a SMAN with 3 sources and 7 intermediate nodes.

subspace $\mathcal{C}_{\text{RS}} = \big\{\big[m(\alpha), m(\alpha^2), \ldots, m(\alpha^N)\big] : \deg\, m(x) < k\big\}$, where $m(x)$ is a polynomial over $\mathbb{F}_q$ of degree $\deg\, m(x)$, and $\alpha \in \mathbb{F}_q$ is a primitive element. The coding scheme operates over a finite field $\mathbb{F}_q$, where q is a power of a prime p, such that $q \geq n+1$. Each message vector $\mathbf{m} = [m_0, \ldots, m_{k-1}]$ is mapped to a message polynomial $m(x) = \sum_{i=0}^{k-1} m_i x^i$, which is then evaluated at N distinct elements $\{\alpha, \alpha, \ldots, \alpha^N\}$ of $\mathbb{F}_q$. The vector of evaluations $\big[m(\alpha), m(\alpha^2), \ldots, m(\alpha^N)\big]$ forms the corresponding codeword. This encoding operation can be described concisely using a generator matrix. The generator matrix of $\mathcal{C}_{\text{RS}}$ is given by $\mathbf{G}_{\text{RS}} \in \mathbb{F}_q^{k\times N}$

$$\mathbf{G}_{\text{RS}} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha^2 & \cdots & \alpha^N \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(k-1)} & \alpha^{2(k-1)} & \cdots & \alpha^{N(k-1)} \end{bmatrix}$$

For the convenience of the reader, we restate the *BCH Bound* which will be used later on. For the proof, see e.g. [6, p.238].

Fact 1 (BCH Bound): Let $p(x) \in \mathbb{F}[x]$ be a non-zero polynomial with t (cyclically) consecutive roots, i.e. $p(\alpha^{j+1}) = \cdots = p(\alpha^{j+t}) = 0$. Then at least $t+1$ coefficients of $p(x)$ are non-zero.

For ease of exposition, and with a slight abuse of terminology, we say that a polynomial $p(x)$ *vanishes* on a set $\mathcal{P} \subseteq \{1, \ldots, N\}$ if $p(x) = \prod_{i\in\mathcal{P}}(x - \alpha^i)$.

IV. Code Construction

As mentioned earlier, each relay node in a SMAN transmits a linear combination of its received symbols. Therefore, the overall coding operation from sources to destination can be represented by a generator matrix $\mathbf{G} \in \mathbb{F}_q^{r_{\mathcal{I}}\times N}$ of a specific structure. The structure is captured by $\mathbf{A}$, which is used to build $\mathbf{G}$ as follows. We replicate the i^{th} row of $\mathbf{A}$ r_i times and then replace the non-zero entries with indeterminates, whose values will be selected later on. We

can write $\mathbf{G}$ as

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \vdots \\ \mathbf{G}_{|\mathcal{S}|} \end{bmatrix}$$

where the jth column of the submatrix $\mathbf{G}_i \in \mathbb{F}_q^{r_i \times N}$ is all zero if S_i is not connected to v_j. For a 3-source SMAN, $\mathbf{G}$ in generic form looks as follows:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{bmatrix} = \left[\begin{array}{c|c|c|c|c|c|c} \times & \mathbf{0} & \mathbf{0} & \mathbf{0} & \times & \times & \times \\ \mathbf{0} & \times & \mathbf{0} & \times & \mathbf{0} & \times & \times \\ \mathbf{0} & \mathbf{0} & \times & \times & \times & \mathbf{0} & \times \end{array}\right]$$

The symbol $\times$ represents a block of indeterminates. For example, the adjacency matrix of the SMAN in Figure 1 is given by

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

It should be noted that the permuting the rows and/or columns of $\mathbf{A}$ still represents the same network. Thus, we can employ such operations when constructing a code for a certain SMAN. Now suppose $z = 1$ and $\mathbf{r} = (3, 1, 1)$. From $\mathbf{A}$, we build $\mathbf{G}$,

$$\mathbf{G} = \left[\begin{array}{ccccccc} g_{1,1} & 0 & 0 & g_{1,4} & g_{1,5} & g_{1,6} & g_{1,7} \\ g_{2,1} & 0 & 0 & g_{2,4} & g_{2,5} & g_{2,6} & g_{2,7} \\ g_{3,1} & 0 & 0 & g_{3,4} & g_{1,5} & g_{3,6} & g_{3,7} \\ \hline 0 & g_{4,2} & g_{4,3} & 0 & 0 & g_{4,6} & g_{4,7} \\ \hline 0 & g_{5,2} & g_{5,3} & g_{5,4} & g_{5,5} & 0 & 0 \end{array}\right] \tag{2}$$

The indeterminates are chosen in way such that the rows of $\mathbf{G}$ span an $r_{\mathcal{I}}$-dimensional subspace $\mathcal{C}$ of $\mathcal{C}_{\text{RS}}$. We call $\mathcal{C}$ a distributed Reed-Solomon code. For each source i, we can straightforwardly find a basis for the vector space of possible rows of $\mathbf{G}_i$ such that it spans an r_i-dimensional subspace of $\mathcal{C}_{\text{RS}}$. The only remaining question is whether for any rate vector $\mathbf{r}$ in the capacity region it is always possible to find vectors for all $\mathbf{G}_i$'s so that they are collectively linearly independent. We can now describe the encoding operation. Let the message of source S_i be represented by a row vector $\mathbf{m}_i = \left[m_1^{(i)}, \ldots, m_{r_i}^{(i)}\right]$, where $m_k^{(i)} \in \mathbb{F}_q$. The j^{th} relay node encodes using the j^{th} column $\mathbf{g}^{(j)}$ of the generator matrix $\mathbf{G}$, and transmits the symbol $[\mathbf{m}_1 \quad \mathbf{m}_2 \quad \ldots \quad \mathbf{m}_{|\mathcal{S}|}]\mathbf{g}^{(j)}$. Let $\mathbf{c}$ denote the overall network codeword $\mathbf{c} = [\mathbf{m}_1 \quad \mathbf{m}_2 \quad \ldots \quad \mathbf{m}_{|\mathcal{S}|}]\mathbf{G}$. The destination node D receives a corrupted version of $\mathbf{c}$, denoted by $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e}$ is z-sparse, and y_i is the symbol received by D through the i^{th} relay link. The following theorem establishes that this is indeed the case for up to three sources.

Theorem 1: For any rate vector $\mathbf{r} \in \mathcal{R}$ in the capacity region of a three-source SMAN, we can construct a distributed Reed-Solomon code.

The proof is constructive, i.e. for a given SMAN along with z, $\mathbf{r}$ and $\mathbf{A}$, we show how to find a transformation matrix $\mathbf{T} \in \mathbb{F}_q^{r_{\mathcal{I}} \times k}$ such that $\mathbf{G} = \mathbf{T}\mathbf{G}_{\text{RS}}$. We can also partition $\mathbf{T}$ such that $\mathbf{G}_i = \mathbf{T}_i\mathbf{G}_{\text{RS}}$:

$$\mathbf{T} = \begin{bmatrix} \mathbf{T}_1 \\ \mathbf{T}_2 \\ \vdots \\ \mathbf{T}_{|\mathcal{S}|} \end{bmatrix}$$

We prove that such a construction is possible by considering four possible cases. Any SMAN with $\mathbf{r} \in \mathcal{R}$ falls precisely under one of these cases. For the first three cases, we show that it is always possible to set the indeterminates in a way such that r_i columns in $\mathbf{G}_i$ form an upper triangular matrix, guaranteeing $\mathsf{rank}(\mathbf{G}) = r_i$. Given the structure of $\mathbf{G}_{\text{RS}}$, we can exactly describe $\mathbf{T}$ by resorting to a polynomial representation of vectors. Effectively, we transform $\mathbf{G}_{\text{RS}}$ into a matrix in row echelon form (up to a permutation of the columns). The fourth case relies on a different strategy, which is treated in a self-contained fashion. We now introduce some needed notation. For all $\mathcal{S}' \subseteq \mathcal{S}$, let $\mathcal{N}_{\mathcal{I}(\mathcal{S}')} \in \mathcal{I}(\mathcal{V})$ denote the set of column indices corresponding to intermediate nodes connected to all $S_i \in \mathcal{S}'$ simultaneously, but not to any other source. We say $\mathcal{N}_{\mathcal{I}(\mathcal{S}')}$ *represents* the columns indexed by its elements. Let $n_{\mathcal{I}(\mathcal{S}')} := |\mathcal{N}_{\mathcal{I}(\mathcal{S}')}|$. For the network in Figure 1, $\mathcal{N}_1 = \{1\}$, and $\mathcal{N}_{1,2} = \{6, 7\}$. Note that the sets $\mathcal{N}_{\mathcal{S}'}$ partition $\mathcal{I}(\mathcal{V})$. Let $\mathcal{Z}_i$ be the set of indices of the columns corresponding to the relay nodes that are not connected to S_i. For example, $\mathcal{Z}_2 = \{1, 4, 5\}$. We will say that $\mathcal{X} \subseteq \mathcal{N}_{\mathcal{I}(\mathcal{S}')}$ is contained in the set of roots of a polynomial $p(x)$ if $p(\alpha^i) = 0$ for all $i \in \mathcal{X}$. We now prove the main theorem by considering each of the following four cases.

Case 1

$$r_1 \leq n_1 \tag{3}$$

$$r_2 \leq n_2 + n_{1,2} \tag{4}$$

Without loss of generality, we assume

$$\begin{aligned} \mathcal{N}_1 &= \{1, \ldots, n_1\} \\ \mathcal{N}_2 &= \{n_1 + 1, \ldots, n_1 + n_2\} \\ \mathcal{N}_{1,2} &= \{n_1 + n_2 + 1, \ldots, n_1 + n_2 + n_{1,2}\} \end{aligned}$$

Given the constraint on r_1 in (3), we can select r_1 columns represented by a subset of $\mathcal{N}_1$ in $\mathbf{G}_1$ and set as the identity matrix (or any other diagonal matrix). Similarly by (4), a collection of r_2 columns represented by a subset of $\mathcal{N}_2 \cup \mathcal{N}_{1,2}$ in $\mathbf{G}_2$ is set as a diagonal matrix. We now move to on to $\mathbf{G}_3$ and select any r_3 columns to set as a diagonal matrix. In essence, the indeterminates of $\mathbf{G}$ are chosen such that it is in row echelon form (up to a permutation of the columns). To show that such matrix can constructed from $\mathbf{G}_{\text{RS}}$, we define

the rows of $\mathbf{T}$ as polynomials that vanish on appropriate sets and have the appropriate degree. Let $t_j^{(1)}(x)$ be a polynomial that vanishes on $\mathcal{Z}_1 \cup \{1, \ldots, r_1\} \setminus j$. The j^{th} row of $\mathbf{T}_1$ is the vector of coefficients of $t_j^{(1)}(x)$ along with extra zeros so that it is composed of k entries. Now, let $t_j^{(2)}(x)$ be a polynomial that vanishes on $\mathcal{Z}_2 \cup \{n_1+1, \ldots, n_1+r_2\} \setminus (n_1+j)$. $\mathbf{T}_2$ is built in the same manner as $\mathbf{T}_1$. To build $\mathbf{T}_3$, choose $t_j^{(3)}(x)$ such that it vanishes on $\mathcal{Z}_3 \cup \{n_1+n_2+n_{1,2}+1, \ldots, n_1+n_2+n_{1,2}+r_3\} \setminus (n_1+n_2+n_{1,2}+j)$. Using this method, we transform $\mathbf{G}_{\text{RS}}$ into $\mathbf{G}$, which is in row echelon form and has no all-zero rows. The cut-set bounds (1) along with the number of roots of $t_j^{(i)}(x)$ imply $\deg\, t_j^{(i)}(x) \leq k-1$. To see this, consider $t_j^{(1)}(x)$ first, which has $|\mathcal{Z}_1|+r_1-1$ roots. Since $r_1 \leq C_1 - 2z$ and $|\mathcal{Z}_1| = N - C_1$, we have $|\mathcal{Z}_1|+r_1-1 \leq N-2z-1 = k-1$. The same argument justifies the claim for $t_j^{(2)}(x)$ and $t_j^{(3)}(x)$. Thus, an appropriate $\mathbf{T}$ can always be found and $\mathsf{rank}(\mathbf{G}) = R_{\mathcal{I}}$, as required.

Case 2

$$r_1 \leq n_1$$

$$r_2 > n_2 + n_{1,2}$$

We make the same assumptions on $\mathcal{N}_1$, $\mathcal{N}_2$ and $\mathcal{N}_{1,2}$. Furthermore,

$$\begin{aligned}\mathcal{N}_{2,3} &= \{n_1+n_2+n_{1,2}+1, \ldots, n_1+n_2+n_{1,2}+n_{2,3}\}\\ \mathcal{N}_{1,2,3} &= \{n_1+n_2+n_{1,2}+n_{2,3}+1, \ldots, n_1+n_2+n_{1,2}+n_{2,3}+n_{1,2,3}\}\end{aligned}$$

We define $t_j^{(1)}(x)$ and $t_j^{(2)}(x)$ as in Case 1. Since $r_2 > n_2+n_{1,2}$, $\mathbf{T}_2$ will affect, in addition to $\mathcal{N}_2 \cup \mathcal{N}_{1,2}$ columns represented by $\mathcal{X}^{(2)} = \mathcal{X}_{2,3}^{(2)} \cup \mathcal{X}_{1,2,3}^{(2)}$, where $\mathcal{X}_{2,3}^{(2)} \subseteq \mathcal{N}_{2,3}$ and $\mathcal{X}_{1,2,3}^{(2)} \subseteq \mathcal{N}_{1,2,3}$, and $x_2 := |\mathcal{X}^{(2)}| = r_2 - (n_2+n_{1,2})$. In other words, $\mathcal{X}_{2,3}^{(2)}$ is the subset of $\mathcal{N}_{2,3}$ contained in $\cup_j \mathcal{L}_j$, where $\mathcal{L}_j$ is the set of roots of $t_j^{(2)}(x)$. In order to have $\mathbf{G}$ in row echelon form, we need to modify $t_j^{(3)}(x)$ such that $\mathbf{T}_3$ also sets the indeterminates in the columns represented by $\mathcal{X}^{(2)}$ in $\mathbf{G}_3$ to zero. Namely, $t_j^{(3)}(x)$ vanishes on $\mathcal{X}^{(2)} \cup \mathcal{Z}_3 \cup \{n_1+n_2+n_{1,2}+x_2+1, \ldots, n_1+n_2+n_{1,2}+x_2+r_3\} \setminus n_1+n_2+n_{1,2}+x_2+j$. Since $t_j^{(1)}(x)$ and $t_j^{(2)}(x)$ are chosen as in Case 1, their degrees are at most $k-1$ as required. For $t_j^{(3)}(x)$, the following relations give the required results:

$$\begin{aligned}\deg\, t_j^{(3)}(x) &= |\mathcal{Z}_3| + x_2 + r_3 - 1\\ &= N - C_3 + r_2 - n_2 - n_{1,2} + r_3 - 1\\ &= n_1 + r_2 + r_3 - 1\\ &\leq n_1 + C_{2,3} - 2z - 1\\ &= N - 2z - 1\\ &= k-1\end{aligned}$$

Case 3

$$r_1 > n_1 \tag{5}$$

$$r_2 > n_2 + n_{1,2} \tag{6}$$

Assume that the elements of the index set $\mathcal{I}(\mathcal{V})$ are ordered as follows: $\mathcal{N}_1, \mathcal{N}_{1,3}, \mathcal{N}_2, \mathcal{N}_{1,2}, \mathcal{N}_{2,3}, \mathcal{N}_3, \mathcal{N}_{1,2,3}$. Given this ordering, the set $\mathcal{N}_{1,2}$ will be used when constructing $\mathbf{G}_2$. Furthemore, the columns represented by $\mathcal{N}_{1,3}$ are exhausted in preference to $\mathcal{N}_{1,2,3}$ when constructing $\mathbf{T}_1$. In other words, the set of roots of $t_j^{(1)}(x)$ will contain (a subset of) $\mathcal{N}_{1,2,3}$ only if $r_1 - (n_1 + n_{1,3}) > 0$. For $\mathbf{T}_2$, a similar reasoning holds by preferring $\mathcal{N}_{2,3}$ over $\mathcal{N}_{1,2,3}$. Our intuition for such ordering is that it utilizes already present zeros in $\mathbf{G}$ to contribute to $\mathsf{rank}(\mathbf{G})$. As before, $t_j^{(1)}(x)$ vanishes on $\mathcal{Z}_1 \cup \{i_1, \ldots, i_{r_1}\} \setminus i_j$, where i_l is the l^{th} element in the ordered set $\mathcal{I}(\mathcal{V}) \setminus \{\mathcal{Z}_1 \cup \mathcal{N}_{1,2}\}$. Note that (6) implies that the set of roots of $t_j^{(2)}(x)$ contains $\mathcal{N}_{1,2}$. Similarly, $t_j^{(2)}(x)$ vanishes on $\mathcal{X}_{1,2,3}^{(1)} \cup \mathcal{Z}_2 \cup \{i_1, \ldots, i_{r_2}\} \setminus i_j$, where i_l is the l^{th} element in the ordered set $\bar{\mathcal{Z}}_2 \setminus \mathcal{X}_{1,2,3}^{(1)}$. Lastly, $t_j^{(3)}(x)$ vanishes on $\mathcal{X}_{1,2,3}^{(1)} \cup \mathcal{X}_{1,2,3}^{(2)} \cup \mathcal{X}_{1,3}^{(1)} \cup \mathcal{X}_{2,3}^{(2)} \cup \mathcal{Z}_3 \cup \{i_1, \ldots, i_{r_3}\} \setminus i_j$ and i_l is the l^{th} element in the ordered set $\bar{\mathcal{Z}}_3 \setminus (\mathcal{X}_{1,2,3}^{(1)} \cup \mathcal{X}_{1,2,3}^{(2)} \cup \mathcal{X}_{1,3}^{(1)} \cup \mathcal{X}_{2,3}^{(2)})$. Before validating our choice of $t_j^{(i)}(x)$, we characterize the sizes of $\mathcal{X}_{1,3}^{(1)}, \mathcal{X}_{2,3}^{(2)}, \mathcal{X}_{1,2,3}^{(1)}, \mathcal{X}_{1,2,3}^{(2)}$:

$$\begin{aligned}
\left|\mathcal{X}_{1,3}^{(1)}\right| &= \mathsf{min}(n_{1,3}, r_1 - n_1) \\
|\mathcal{X}_{2,3}^{(2)}| &= \mathsf{min}(n_{2,3}, r_2 - (n_2 + n_{1,2})) \\
|\mathcal{X}_{1,2,3}^{(1)}| &= r_1 - n_1 - |\mathcal{X}_{1,3}^{(1)}| \\
|\mathcal{X}_{1,2,3}^{(2)}| &= r_2 - (n_2 + n_{1,2}) - |\mathcal{X}_{2,3}^{(2)}|
\end{aligned}$$

We now bound the degree of $t_j^{(i)}(x)$. Using the same argument as in Case 1, $\mathsf{deg}\ t_j^{(1)}(x) \leq k - 1$. Now we consider $t_j^{(2)}(x)$. Assume $\left|\mathcal{X}_{1,3}^{(1)}\right| = n_{1,3}$:

$$\begin{aligned}
\mathsf{deg}\ t_j^{(2)}(x) &= |\mathcal{X}_{1,2,3}^{(1)}| + |\mathcal{Z}_2| + r_2 - 1 \\
&= r_1 - n_1 - n_{1,3} + N - C_2 + r_2 - 1 \\
&= r_1 + r_2 + n_3 - 1 \\
&\leq C_{1,2} - 2z + n_3 - 1 \\
&= k - 1
\end{aligned}$$

The same approach holds when justifying the claim for $t_j^{(3)}(x)$. What remains to show is that $|\mathcal{X}_{1,2,3}^{(1)}| + |\mathcal{X}_{1,2,3}^{(2)}| \leq n_{1,2,3}$. Assume $|\mathcal{X}_{1,2,3}^{(1)}| = r_1 - n_1 - n_{1,3}$, $|\mathcal{X}_{1,2,3}^{(2)}| = r_2 - (n_2 + n_{1,2}) - n_{2,3}$. This is justified since columns represented by elements in $\mathcal{N}_{1,2,3}$ are used in the construction of $\mathbf{G}_1$ and $\mathbf{G}_2$ only if these assumptions hold. By assumption on $\mathbf{r}$, $r_1 + r_2 \leq C_{1,2} - 2z \leq C_{1,2} = n_1 + n_2 + n_{1,2} + n_{1,3} + n_{2,3} + n_{1,2,3}$. Rearranging this to $r_1 - n_1 - n_{1,3} + r_2 - (n_2 + n_{1,2}) - n_{2,3} \leq n_{1,2,3}$ and noticing that the left hand side of the inequality is equal to $|\mathcal{X}_{1,2,3}^{(1)}| + |\mathcal{X}_{1,2,3}^{(2)}|$ yields the result.

Case 4

$$r_1 > n_1$$

$$r_2 \leq n_2 + n_{1,2}$$

This case is approached differently. First, we permute the $\mathbf{G}_i$'s to recast the problem such that it falls under Case 1, 2 or 3. If this is possible, then we basically construct the code as earlier. Otherwise, for all $i \neq j$,

$$r_i > n_i \tag{7}$$

$$r_i \leq n_i + n_{i,j} \tag{8}$$

We will assume that the columns of $\mathbf{G}$ are ordered in the following manner.

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{bmatrix} = \left[\begin{array}{ccc|ccc|c} \times & \mathbf{0} & \mathbf{0} & \times & \times & \mathbf{0} & \times \\ \mathbf{0} & \times & \mathbf{0} & \times & \mathbf{0} & \times & \times \\ \mathbf{0} & \mathbf{0} & \times & \mathbf{0} & \times & \times & \times \end{array}\right]$$

For this case, we place an identity of size n_i in the submatrix that corresponds to the columns represented by $\mathcal{N}_i$ and the block $\mathbf{G}_i$. We permute the rows of $\mathbf{G}$ to obtain the following:

$$\mathbf{G} = \left[\begin{array}{ccc|ccc|c} \mathbf{I} & \mathbf{0} & \mathbf{0} & \times & \times & \mathbf{0} & \times \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \times & \mathbf{0} & \times & \times \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \times & \times & \times \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \times & \times & \mathbf{0} & \times \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \times & \mathbf{0} & \times & \times \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \times & \times & \times \end{array}\right] \tag{9}$$

The blocks of columns of $\mathbf{G}$ have sizes $n_1, n_2, n_3, n_{1,2}, n_{1,3}, n_{2,3}, n_{1,2,3}$, while the blocks of rows have sizes $n_1, n_2, n_3, r_1 - n_1, r_2 - n_2, r_3 - n_3$.

We will construct a matrix $\mathbf{T}$ (with dimensions $R_{\mathcal{I}} \times k$), partitioned into two row-blocks, that will transform the generator matrix of a $[N, k, d]$ RS code $\mathbf{G}_{\text{RS}}$ to one whose mask is given by $\mathbf{G}$ in (9).

$$\mathbf{G} = \mathbf{T}\mathbf{G}_{\text{RS}} = \begin{bmatrix} \mathbf{S} \\ \mathbf{V} \end{bmatrix} \mathbf{G}_{\text{RS}} = \left[\begin{array}{c|c} \mathbf{I} & \hat{\mathbf{G}}_{\mathbf{1}} \\ \hline \mathbf{0} & \hat{\mathbf{G}}_{\mathbf{2}} \end{array}\right] = \begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{G}} \end{bmatrix} \tag{10}$$

Note that $\mathbf{S}$ has $\bar{n} := \sum n_i$ rows and $\mathbf{V}$ has $R' := \sum r'_i$ rows, where $r'_i = r_i - n_i$. Constructing $\mathbf{S}$ is straightforward and we only focus on $\mathbf{V}$.

Construction of $\mathbf{V}$*:* As before, the construction boils down to finding polynomials with the appropriate roots, i.e. roots corresponding to the zeros in $\hat{\mathbf{G}}$. Each of these polynomials will have $N - (1 + 2z)$ roots. Using the coefficients of these polynomials as the rows of $\mathbf{V}$ will provide the required result. Let $c(x) = \prod_{i=1}^{\bar{n}}(x - \alpha^i)$. This polynomial will produce the all-zero columns of $\hat{\mathbf{G}}$, namely the columns represented by $\mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$. Now

consider the polynomial $p(x) = \prod_{i\in\mathcal{P}}(x-\alpha^i)$ which vanishes on $\mathcal{P} = \{n_{1,2}+n_{1,3}+\bar{n}+1, n_{1,2}+n_{1,3}+\bar{n}+2, \ldots, n_{1,2}+n_{1,3}+k-1\}$, and form the polynomial $v(x) = c(x)p(x)$. Defining the row vector $[v(\alpha^i)]$, $i = 1, \ldots, N$ yields the first row of $\hat{\mathbf{G}}$ in (10).

To proceed with the construction,we define the following sets:

$$\begin{aligned}
\mathcal{J}_1 &= \{0, 1, \ldots, r_1' - 1\} \\
\mathcal{J}_2 &= \{n_{1,3}, n_{1,3}+1, \ldots, n_{1,3}+r_2'-1\} \\
\mathcal{J}_3 &= \{n_{1,3}+n_{1,2}, n_{1,3}+n_{1,2}+1, \ldots, n_{1,3}+n_{1,2}+r_3'-1\}
\end{aligned}$$

We partition $\mathbf{V}$ as follows:

$$\mathbf{V} = \begin{bmatrix} \mathbf{V}_1 \\ \mathbf{V}_2 \\ \mathbf{V}_3 \end{bmatrix}$$

The j^{th} row of $\mathbf{V}_i$ (with dimensions $r_i' \times k$) corresponds to the coefficients of $v_j^{(i)}(x) = c(x)p(\alpha^j x)$, where $j \in \mathcal{J}_i$. Using this method, $c(x)$ still produces the zeros required for the all zero block. The remaining zeros in each row are produced by $p(\alpha^j x)$, which basically shifts the location of the roots of $p(x)$ by j positions to the left appropriately. Since $p(x)$ has $t = k - \bar{n} - 1$ roots, a row in $\hat{\mathbf{G}}_2$ with a requirement of, say, $n_{2,3}$ zeros will have an excess of $t - n_{2,3}$ zeros. Nonetheless, the weight of every row of $\hat{\mathbf{G}}$ is still at least $1 + 2z$. Now, we proceed to show that $\mathbf{V}$ is full rank.

First, we need that the $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ sets are pairwise disjoint. Note the elements in each $\mathcal{J}_i$ are increasing. By the constraints (8), $r_1 \leq n_1 + n_{1,3}$. Thus $r_1' - 1 < n_{1,3}$ and $\mathcal{J}_1 \cap \mathcal{J}_2 = \emptyset$. A similar argument implies $\mathcal{J}_2 \cap \mathcal{J}_3 = \emptyset$.

Now, we show that the polynomials $v_j^{(i)}(x)$ are linearly independent. Note that this is true if and only if the polynomials $p(\alpha^j x)$ are linearly independent. Therefore, we focus on the latter.

V. Rank of $\mathbf{V}$

Write $p(x) = \sum_{l=0}^{t} p_l x^l$ and $p(\alpha^j x) = \sum_{l=0}^{t} p_l \alpha^{jl} x^l$. Consider the matrix $\mathbf{P}$ formed by the coefficients of $p(\alpha^j x)$, $j \in \cup_i \mathcal{J}_i$

$$\mathbf{P} = \begin{bmatrix} p_0 & p_1\alpha^{j_1} & \ldots & p_t\alpha^{j_1 t} \\ p_0 & p_1\alpha^{j_2} & \ldots & p_t\alpha^{j_2 t} \\ \vdots & \vdots & \ddots & \vdots \\ p_0 & p_1\alpha^{j_{R'}} & \ldots & p_t\alpha^{j_{R'} t} \end{bmatrix}$$

The matrix $\mathbf{P}$ (dimensions $R' \times t+1$) is never a tall matrix since by the rate region $R' \leq t+1$. Consider the

matrix $\hat{\mathbf{P}}$ which is formed from the first R' columns of $\mathbf{P}$. Writing out the determinant of $\hat{\mathbf{P}}$ yields

$$\begin{aligned}\mathsf{det}(\hat{\mathbf{P}}) &= \begin{vmatrix} p_0 & p_1\alpha^{j_1} & \dots & p_{R-1}\alpha^{j_1(R'-1)} \\ p_0 & p_1\alpha^{j_2} & \dots & p_{R-1}\alpha^{j_2(R'-1)} \\ \vdots & \vdots & \ddots & \vdots \\ p_0 & p_1\alpha^{j_{R'}} & \dots & p_{R'-1}\alpha^{j_{R'}(R'-1)} \end{vmatrix} \\ &= \prod_{i=0}^{R'-1} p_i \begin{vmatrix} 1 & \alpha^{j_1} & \dots & \alpha^{j_1(R'-1)} \\ 1 & \alpha^{j_2} & \dots & \alpha^{j_2(R'-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{j_{R'}} & \dots & \alpha^{j_{R'}(R'-1)} \end{vmatrix}\end{aligned}$$

Using the BCH bound, we establish that all p_i's are nonzero. Therefore $\mathsf{det}(\hat{\mathbf{P}})$ is equal to the determinant of the Vandermonde matrix with defining set $\{\alpha^{j_1}, \dots, \alpha^{j_{R'}}\}$, multiplied by a non-zero scalar. As it was established earlier, the elements $\{\alpha^{j_1}, \dots, \alpha^{j_{R'}}\}$ are all distinct in $\mathbb{F}_q$.

Therefore, $\mathbf{P}$ is full rank implying that the polynomials $v_j^{(i)}(x)$ are linearly independent and so $\mathsf{rank}(\hat{\mathbf{G}}) = R'$. We also observe that $\mathsf{rank}(\mathbf{G}) = \mathsf{rank}(\mathbf{X}) + \mathsf{rank}(\hat{\mathbf{G}}) = \bar{n} + R' = R_{\mathcal{I}}$. Thus $\mathbf{G}$ is full rank.

VI. Decoding Details

In essence, we have used a subcode of a RS code to correct errors in a SMAN. Generally speaking, any decoding algorithm designed for *evaluation-based* construction of RS-codes can be used to decode the received symbols to a valid codeword $\hat{\mathbf{c}}$. However, this doesn't imply that the we can immediately *de-map* the codeword to the original message $\mathbf{m}$. Nonetheless, if we were to use a decoder that produces a valid message $\hat{\mathbf{m}}_{\text{RS}}$ such that $\hat{\mathbf{c}} = \hat{\mathbf{m}}_{\text{RS}}\mathbf{G}_{\text{RS}}$, then we can obtain an estimate of the transmitted message vector $\hat{\mathbf{m}}$ easily using our knowledge of $\mathbf{T}$.

Thus, we use the Berlekamp-Welch decoder as described by Gemmell and Sudan in [7]. Assuming at most z errors occur, we recover the unique $\mathbf{m}_{\text{RS}}$ such that $\mathbf{c} = \mathbf{m}\mathbf{G} = \mathbf{m}\mathbf{T}\mathbf{G}_{\text{RS}} = \mathbf{m}_{\text{RS}}\mathbf{G}_{\text{RS}}$. Since $\mathbf{T}$ has full row rank, it follows that $\mathbf{m}_{\text{RS}} = \mathbf{m}\mathbf{T}$. Next let $\tilde{\mathbf{T}}$ be a matrix of $R_{\mathcal{I}}$ columns of $\mathbf{T}$ such that it is invertible[1]. We can now recover $\mathbf{m}$ since $\tilde{\mathbf{m}}_{\text{RS}}\tilde{\mathbf{T}}^{-1} = \mathbf{m}$, where $\tilde{\mathbf{m}}_{\text{RS}}$ is a subvector of $\mathbf{m}_{\text{RS}}$ with length $R_{\mathcal{I}}$, corresponding to the columns of $\mathbf{T}$ selected in $\tilde{\mathbf{T}}$.

VII. Example

In this section, we show how to construct a DRS code for the SMAN in Figure 1. Assume $\mathbf{r} = (3, 1, 1)$ and $z = 1$. From here, it follows that the construction of Case 4 should be used. The constituent code is a $[7, 5, 3]$ RS code over $\mathbb{F}_8$ with primitive polynomial $x^3 + x + 1$. The poynomials and sets of interest are tabulated below:

[1]If the problem instance falls under Case 4, then we know that the first $R_{\mathcal{I}}$ columns are linearly independent. Otherwise, $\mathbf{T}$ can be reduced to row echelon form using Gaussian elimination, and then we select the pivot columns.

$$c(x) = (x - \alpha)$$
$$p(x) = (x - \alpha^6)(x - \alpha^7)(x - \alpha^8)$$
$$\mathcal{J}_1 = \{0, 1\}$$
$$\mathcal{J}_2 = \{2\}$$
$$\mathcal{J}_3 = \{4\}$$

Next we can evaluate $v_j^{(i)}(x)$ for $j \in \mathcal{J}_i$ and $i = 1, 2, 3$ to obtain

$$\mathbf{V} = \begin{bmatrix} \alpha & \alpha^4 & 1 & \alpha^2 & 1 \\ \alpha & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 \\ \alpha & 0 & 1 & \alpha^3 & \alpha^6 \\ \alpha & \alpha^6 & \alpha^5 & \alpha & \alpha^5 \end{bmatrix}$$

The polynomial $s(x)$ corresponding to $\mathbf{S}$ is $s(x) = \frac{(x-\alpha^6)(x-\alpha^7)}{(\alpha-\alpha^6)(\alpha-\alpha^7)}$. The scaling factor forces $s(\alpha) = 1$. Finally, we have the transformation matrix $\mathbf{T}$ and the corresponding $\mathbf{G}$:

$$\mathbf{T} = \left[\begin{array}{ccccc} \alpha^5 & \alpha & \alpha^6 & 0 & 0 \\ \hline \alpha & \alpha^4 & 1 & \alpha^2 & 1 \\ \alpha & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 \\ \alpha & 0 & 1 & \alpha^3 & \alpha^6 \\ \alpha & \alpha^6 & \alpha^5 & \alpha & \alpha^5 \end{array}\right]$$

$$\mathbf{G} = \left[\begin{array}{ccccccc} 1 & \alpha^5 & \alpha^4 & 1 & \alpha^4 & \mathbf{0} & \mathbf{0} \\ 0 & 1 & \alpha^5 & \alpha^5 & \alpha^3 & \mathbf{0} & \mathbf{0} \\ 0 & \alpha^2 & \alpha^3 & \alpha^6 & 0 & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & 1 & \alpha^4 & \mathbf{0} & \mathbf{0} & 0 & \alpha^6 \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & \alpha^2 & \alpha^3 & \alpha^6 \end{array}\right]$$

The required zeros are in boldface. Note that $\mathbf{G}$ has the same form of the following mask, which is a valid permutation of the generic mask in (2).

$$\mathbf{G} = \left[\begin{array}{ccccccc} g_{1,1} & g_{1,2} & g_{1,3} & g_{1,4} & g_{1,5} & \mathbf{0} & \mathbf{0} \\ g_{2,1} & g_{2,2} & g_{2,3} & g_{2,4} & g_{2,5} & \mathbf{0} & \mathbf{0} \\ g_{3,1} & g_{3,2} & g_{1,3} & g_{3,4} & g_{3,5} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & g_{4,2} & g_{4,3} & \mathbf{0} & \mathbf{0} & g_{4,6} & g_{4,7} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & g_{5,4} & g_{5,5} & g_{5,6} & g_{5,7} \end{array}\right]$$

VIII. Conclusion

We have proposed a distributed Reed-Solomon coding scheme for simple multiple access networks, with much lower decoding complexity compared to existing constructions for the general multiple access network error correction problem. The field size scales linearly with the length of the code as opposed to exponentially with the number of sources. We show that it achieves the full capacity region for up to three sources. It remains as further work to determine whether it can achieve the full capacity region for networks with more than three sources; our proof for three sources does not extend straightforwardly since the method of classifying the problem depending on the rate vector results in an exponentially growing number of cases.

References

[1] H. Yao, T. Ho, and C. Nita-Rotaru, "Key agreement for wireless networks in the presence of active adversaries," in *Proc. IEEE Asilomar Conf. on Signals, Sys. and Comp.*, 2011.

[2] T. Dikaliotis, T. Ho, S. Jaggi, S. Vyetrenko, H. Yao, M. Effros, J. Kliewer, and E. Erez, "Multiple access network information-flow and correction codes," *Special issue of the IEEE Transactions on Information Theory dedicated to the scientific legacy of Ralf Koetter*, vol. 57, no. 2, pp. 1067–1079, 2011.

[3] S. H. Dau, W. Song, Z. Dong, and C. Yuen, "Balanced Sparsest generator matrices for MDS codes," in *Inf. Theory Proc. (ISIT), 2013 IEEE Int. Symp.*, 2013, pp. 1889–1893.

[4] S. El Rouayheb, A. Sprintson, and P. Sadeghi, "On coding for cooperative data exchange," in *Inf. Theory Work. (ITW), 2010 IEEE*, 2010, pp. 1–5.

[5] I. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, 1960.

[6] R. J. McEliece, *The Theory of Information and Coding*. Cambridge University Press, 2002.

[7] P. Gemmell and M. Sudan, "Highly resilient correctors for polynomials," *Inf. Process. Lett.*, vol. 43, no. 4, pp. 169–174, Sep. 1992.